SN 10/588,608

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002007215 A**

(43) Date of publication of application: **11.01.02**

(51) Int. Cl **G06F 12/14**

(21) Application number: **2000181546**

(22) Date of filing: **16.06.00**

(71) Applicant: **FUJITSU KIDEN LTD**

(72) Inventor: **KASAHARA YASUSHI**
HASEGAWA AKIRA
OBA JUNICHIRO
SATO MAKOTO
SAWADA ICHIRO
SAITO SATOSHI

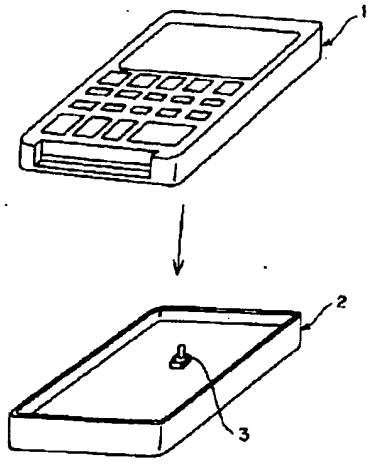
(54) **FORGERY-PREVENTING DEVICE FOR ELECTRONIC EQUIPMENT**

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a forgery-preventing device which effectively prevents electronic equipment from being forged, using a simple constitution.

SOLUTION: A switch 3 which turns on only when an upper cover 1 is closed to a lower cover 2 is provided as a means for detecting the housing of the electronic equipment in an opened state (separation of the upper cover 1 and lower cover 2). When the electronic equipment is used normally, the lower cover 2 is closed to the upper cover 1, so the switch 3 is depressed by the upper cover 1 to maintain the 'on' state. If the electronic equipment is forged illegally, the upper cover 1 is opened from the lower cover 2, so the switch 3 leaves the upper cover 1 to turn off. If the 'off' state of the switch 3 (i.e., opening of the covers 1 and 2) is detected, it is discriminated that the electronic equipment has been forged, and the functions of the electronic equipment are stopped. Here, the functions are stopped, for example, by destroying memory data by turning off a backup power source and detecting the resulting memory check error.

本発明の一実施の形態に係る改ざん防止装置を
組み込んだ電子機器を概略的に示した外観斜視図



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－7215
（P2002－7215A）
(43)公開日　平成14年１月11日(2002.1.11)

(51)Int.Cl.'	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｄ　５Ｂ０１７

審査請求　未請求　請求項の数12　ＯＬ　（全６頁）

(21)出願番号　特願2000－181546(P2000－181546)

(22)出願日　平成12年６月16日(2000.6.16)

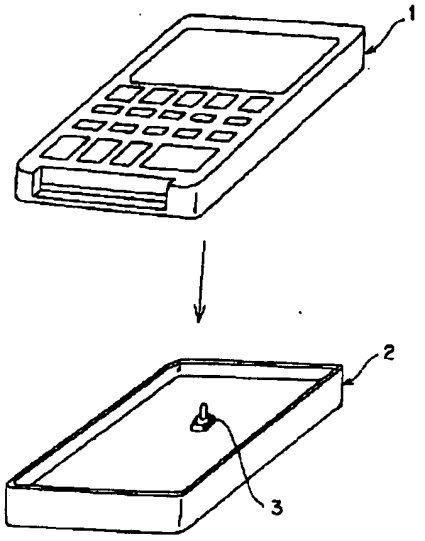
(71)出願人　000237639
富士通機電株式会社
東京都稲城市矢野口1776番地
(72)発明者　笠原　泰
東京都稲城市矢野口1776番地　富士通機電株式会社内
(72)発明者　長谷川　亮
東京都稲城市矢野口1776番地　富士通機電株式会社内
(74)代理人　100074099
弁理士　大菅　義之　（外１名）

最終頁に続く

(54)【発明の名称】　電子機器の改ざん防止装置

(57)【要約】
【課題】簡単な構成で電子機器の改ざんを有効に防止することの可能な改ざん防止装置を提供する。
【解決手段】電子機器の筐体の開放（上部カバー１と下部カバー２との分離）を検出するための手段として、下部カバー２に対して上部カバー１を閉じた状態でのみオンするスイッチ３を設ける。電子機器が正常に使用されている場合は、下部カバー２に対し上部カバー１が閉じた状態にあるため、スイッチ３は上部カバー１により押下されてオン状態を維持する。一方、電子機器が不正に改ざんされる場合は、下部カバー２に対して上部カバー１が開放されることになるため、スイッチ３は上部カバー１との当接状態が外れてオフ状態となる。スイッチ３のオン、オフを検出し、もしオフ状態（すなわちカバー１、２の開放）が検出された場合は、改ざんされたものと判断して、電子機器の機能停止を実行する。電子機器の機能停止は、例えば、バックアップ電源を遮断すること等によりメモリデータを破壊し、それによるメモリチェックエラーを検出すること等により行う。

本発明の一実施の形態に係る改ざん防止装置を組み込んだ電子機器を概略的に示した外観斜視図



1

【特許請求の範囲】

【請求項１】電子機器に組み込まれた改ざん防止装置であって、

前記電子機器の改ざんを検出する検出手段と、

該検出手段により改ざんが検出された場合、前記電子機器の機能を停止させる機能停止手段と、

を備えることを特徴とする改ざん防止装置。

【請求項２】前記検出手段は、前記電子機器の筐体が開放されることによりオン又はオフするスイッチを有し、該スイッチのオン又はオフを前記改ざんとして前記電子機器の回路部で検出することを特徴とする請求項１記載の改ざん防止装置。

【請求項３】前記検出手段は、前記電子機器の筐体が開放されることにより切断されるヒューズを有し、該ヒューズの切断を前記改ざんとして前記電子機器の回路部で検出することを特徴とする請求項１記載の改ざん防止装置。

【請求項４】前記検出手段は、前記電子機器の筐体が開放されることにより抵抗値の変化する内部抵抗を有し、該内部抵抗の抵抗値の変化を前記改ざんとして前記電子機器の回路部で検出することを特徴とする請求項１記載の改ざん防止装置。

【請求項５】前記機能停止手段は、前記検出手段で改ざんが検出された場合に前記電子機器のメモリデータを破壊する手段と、該メモリデータの破壊によるメモリチェックエラーを検出して前記電子機器の機能を停止させる手段とを有することを特徴とする請求項１乃至４のいずれか１つに記載の改ざん防止装置。

【請求項６】前記メモリデータを破壊する手段は、前記電子機器のバックアップ電源を遮断することにより前記メモリデータを破壊することを特徴とする請求項５記載の改ざん防止装置。

【請求項７】前記メモリデータを破壊する手段は、前記電子機器の電源回路をショートさせることにより前記メモリデータを破壊することを特徴とする請求項５記載の改ざん防止装置。

【請求項８】前記メモリデータを破壊する手段は、前記電子機器内の回路素子を逆電圧で破壊することにより前記メモリデータを破壊することを特徴とする請求項５記載の改ざん防止装置。

【請求項９】前記機能停止手段は、前記検出手段で改ざんが検出された場合に前記電子機器の時計データを破壊する手段と、該時計データの破壊による時刻チェックエラーを検出して前記電子機器の機能を停止させる手段とを有することを特徴とする請求項１乃至４のいずれか１つに記載の改ざん防止装置。

【請求項10】前記時計データを破壊する手段は、前記電子機器のバックアップ電源を遮断することにより前記時計データを破壊することを特徴とする請求項９記載の改ざん防止装置。

2

【請求項11】前記時計データを破壊する手段は、前記電子機器の電源回路をショートさせることにより前記時計データを破壊することを特徴とする請求項９記載の改ざん防止装置。

【請求項12】前記時計データを破壊する手段は、前記電子機器内の回路素子を逆電圧で破壊することにより前記時計データを破壊することを特徴とする請求項９記載の改ざん防止装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えば携帯用端末機器やカード読み取り装置等のような各種電子機器が悪意の第三者により改ざんされるのを防止する改ざん防止装置に関する。

【０００２】

【従来の技術、及び発明が解決しようとする課題】従来、上述したような電子機器が盗難等の被害に会った場合、その電子機器内に蓄積された重要データが盗まれて悪用されてしまう、といった危険性が高かった。

【０００３】また、電子機器の内部に盗聴回路が仕掛けられ、重要データが盗用されるといった被害も生じていた。このような被害は、特に、クレジットカード等のカードの読み取り装置において多く生じていた。

【０００４】従来は、このように悪意の第三者により電子機器が改ざんされる危険性が大きかったが、これを簡単な構成で有効に防止する手段が存在しなかった。本発明は、上記従来の問題点に鑑み、簡単な構成で電子機器の改ざんを有効に防止することの可能な改ざん防止装置を提供することを課題とする。

【０００５】

【課題を解決するための手段】本発明は、上記課題を解決するため、以下のように構成する。すなわち、本発明の改ざん防止装置は、改ざんの対象となる電子機器に組み込んで使用されるものであって、上記電子機器の改ざんを検出する検出手段と、この検出手段により改ざんが検出された場合に上記電子機器の機能を停止させる機能停止手段と、を備えることを特徴とするものである。

【０００６】このような構成からなる本発明の改ざん防止装置の組み込まれた電子機器によれば、もしこの電子機器が改ざんされた場合であっても、この改ざんを上記検出手段が検出し、これにより上記機能停止手段が電子機器を機能停止させることになる。その結果、悪意の第三者が電子機器に改ざんを加えて重要データを不法に盗み出そうとしても、その改ざんの際に電子機器の機能が停止してしまい、簡単に復旧させることができなくなるため、データの盗用を有効に防止することが可能となる。

【０００７】以上の構成において、上記検出手段としては、電子機器の改ざんを検出可能な各種構成を採用可能であり、例えば、（１）電子機器の筐体（カバー）が開

放されることによりオン又はオフするスイッチを有し、このスイッチのオン又はオフを"改ざん"として電子機器の回路部で検出するような構成、（２）電子機器の筐体が開放されることにより切断されるヒューズを有し、このヒューズの切断を"改ざん"として電子機器の回路部で検出するような構成、（３）電子機器の筐体が開放されることにより抵抗値の変化する内部抵抗を有し、この内部抵抗の抵抗値の変化を"改ざん"として電子機器の回路部で検出するような構成等、が望ましい一例として考えられる。

【０００８】また、上記機能停止手段としては、上記検出手段による改ざんの検出に基づいて電子機器の機能を停止させることの可能な各種構成を採用可能であり、例えば、（１）上記検出手段で改ざんが検出された場合に電子機器のメモリデータを破壊する手段と、このメモリデータの破壊によるメモリチェックエラーを検出して電子機器の機能を停止させる手段とを有する構成や、

（２）上記検出手段で改ざんが検出された場合に電子機器の時計データを破壊する手段と、この時計データの破壊による時刻チェックエラーを検出して電子機器の機能を停止させる手段とを有する構成等、が望ましい一例として考えられる。

【０００９】なお、上記のメモリデータを破壊する手段や時計データを破壊する手段としては、例えば、電子機器のバックアップ電源を遮断する構成、電子機器の電源回路をショートさせる構成、電子機器内の回路素子を逆電圧で破壊する構成等が、望ましい一例として考えられるが、これらに限定されるものではない。

【００１０】

【発明の実施の形態】以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。

＜本発明の一実施の形態＞図１は、本発明の一実施の形態に係る改ざん防止装置を組み込んだ電子機器を概略的に示した外観斜視図である。

【００１１】この電子機器は、携帯用の端末機器を一例として示したものであり、その筐体が上部カバー１と下部カバー２とから構成される場合である。これらカバー１、２は通常は一体化された状態に結合されており、内部の回路に容易に操作を加えることはできないようになっている。この電子機器に対して改ざんを加えるには、上部カバー１と下部カバー２とを分離しなければならない。

【００１２】そこで、本実施の形態では、図１に明らかなように、電子機器の筐体の開放（すなわち上部カバー１と下部カバー２との分離）を検出するための手段として、下部カバー２に対して上部カバー１を閉じた状態でのみオンするスイッチ３を設けてある。

【００１３】図２は上記スイッチ３の動作を説明する図であって、同図（ａ）は上部カバー１を閉じた状態、同図（ｂ）は上部カバー１を開いた状態である。電子機器

が正常に使用されている場合は、下部カバー２に対し上部カバー１が閉じた状態にあるため、図２（ａ）に示すように、スイッチ３は上部カバー１内面の凸部１ａにより押下されてオン状態を維持する。一方、電子機器が不正に改ざんされる場合は、下部カバー２に対して上部カバー１が開放されることになるため、図２（ｂ）に示すように、スイッチ３は上部カバー１との当接状態が外れてオフ状態となる。

【００１４】スイッチ３のオン、オフ状態は、図３に示すように、電子機器内に備わった回路部４で検出され、カバー１、２の開閉が判断される。すなわち、図３（ａ）に示すようにスイッチ３がオン状態であれば、カバー１、２は閉じた状態にあり、正常に使用されていると判断する。一方、図３（ｂ）に示すようにスイッチ３がオフ状態に切り換わったとすれば、カバー１、２が開いた状態となり、改ざんされたものと判断する。

【００１５】上記回路部４は、上記のようにしてスイッチ３のオン、オフを検出し、もしオフ状態（すなわちカバー１、２の開放）が検出された場合は、上記のように改ざんされたものと判断して、電子機器の機能停止を実行する。

【００１６】このような機能停止の手段として、回路部４は、スイッチ３のオフ検出により電子機器のバックアップ電源を遮断することでメモリデータを破壊し、このメモリデータの破壊によるメモリチェックエラーを検出して電子機器を機能停止させる。

【００１７】なお、バックアップ電源の遮断は、例えば、バックアップ電源からの電流経路上にトランジスタ等のスイッチング素子を設けておき、スイッチ３のオフにより上記スイッチング素子をオフするような回路ロジックを組んでおくこと等により実現可能である。このようなバックアップ電源の遮断により、メモリ中のデータが破壊される。

【００１８】そして、例えば電子機器の立ち上がりの際等にメモリチェックを行うように予めプログラミングしておくことで、上記のメモリデータの破壊によるメモリチェックエラーが検出されることになり、その結果、電子機器の機能が停止される。

【００１９】なお、上述したような機能を有する回路部４は、電子機器に元々備わった回路部における回路ロジックやプログラムに若干の修正・変更を加えるだけで実現可能である。

【００２０】従って、以上に述べた本実施の形態によれば、もし電子機器が悪意の第三者により改ざんされた場合であっても、この改ざんをスイッチ３で検出し、これにより電子機器を機能停止させることができる。その結果、悪意の第三者が電子機器から重要データを不法に盗み出すのを、有効に防止することができる。

＜その他の実施の形態＞本発明は、上記実施の形態に限定されるものではなく、請求項１に記載した範囲内にお

いて、種々の構成を採用可能である。例えば、以下のような構成変更も可能である。

【００２１】（１）改ざんを検出する手段として、上記実施の形態ではスイッチ３を採用したが、その他の構成も採用可能である。例えば、電子機器の筐体が開放されることにより切断されるヒューズを有し、このヒューズの切断を"改ざん"として電子機器の回路部で検出するような構成であってもよい。この場合、ヒューズを切断するための構成としては、例えば、筐体が開放されることによりヒューズに過大な電流が流れるような回路を組んでおく等、各種の構成を採用可能である。

【００２２】或いは、電子機器の筐体が開放されることにより抵抗値の変化する内部抵抗を有し、この内部抵抗の抵抗値の変化を"改ざん"として電子機器の回路部で検出するような構成であってもよい。この場合は、例えば、筐体が閉じた状態でのみ導通する導電部を上下のカバー間に設けておき、これらカバーが開放することにより上記導電部の導通が遮断されるような回路構成としておくことで、導通の遮断による内部抵抗値の変化を"改ざん"として検出可能である。

【００２３】（２）電子機器の機能停止を行う手段として、上記実施の形態ではバックアップ電源を遮断してメモリデータを破壊する構成を採用したが、その他の構成も採用可能である。

【００２４】例えば、改ざんが検出された場合に電子機器の時計データを破壊するようにし、この時計データの破壊による時刻チェックエラーを検出して電子機器の機能を停止させる構成であってもよい。

【００２５】なお、上記のメモリデータを破壊する手段や時計データを破壊する手段としては、上述したように電子機器のバックアップ電源を遮断する構成の他にも、例えば、電子機器の電源回路をショートさせる構成や、電子機器内の回路素子を逆電圧で破壊する構成等、各種の構成が採用可能である。

【００２６】なお、電源回路をショートさせる構成は、例えば、改ざんの検出によりオンするスイッチング素子を電源回路の所要箇所に設けておくこと等により実現可能である。

【００２７】また、回路素子を逆電圧で破壊する構成は、その破壊によりメモリデータや時計データの破壊を生じさせうるような何らかの回路素子に対して、改ざんの検出により逆電圧を印加すること等により実現可能である。ここで、逆電圧の印加は、適当に回路ロジックを組むこと等により可能である。

【００２８】（３）図１においては、ただ１個のスイッチ３のみを採用したが、適当な箇所に複数のスイッチを設けてもよい。例えば、電子機器の上下カバーが図１のような全開する構成ではなく、部分的に開放する構成である場合は、各部分毎にスイッチを設けてもよい。

【００２９】勿論、回路的に問題がなければ、スイッチ３を上部カバー１に設けた構成であってもよく、その取付箇所も任意である。また、カバーを閉じた時にオフし、開けた時にオンするスイッチであってもよい。

【００３０】スイッチとしては、各種タイプのものを採用可能であり、例えばホール素子やマイクロスイッチ等であってもよい。

（４）上記実施の形態では、本発明の改ざん防止装置を携帯用端末機器に組み込んだ場合について述べたが、本発明はこのような携帯用端末機器に対してのみならず、改ざんの可能性を有する様々な電子機器に適用して有効である。

【００３１】

【発明の効果】本発明によれば、電子機器が改ざんされた場合、その改ざんを検出して電子機器を機能停止させることができるので、非常に簡単な構成であるにもかかわらず、悪意の第三者が電子機器の重要データを盗み出すのを極めて有効に防止することができる。

【図面の簡単な説明】

【図１】本発明の一実施の形態に係る改ざん防止装置を組み込んだ電子機器を概略的に示した外観斜視図である。

【図２】図１に示したスイッチ３の動作を説明する図であって、（ａ）は上部カバー１を閉じた状態であり、（ｂ）は上部カバー１を開いた状態である。

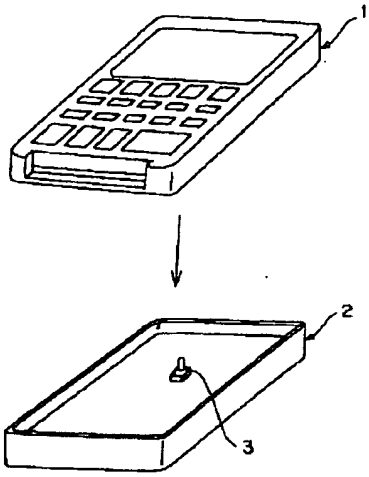
【図３】図１に示したスイッチ３と電子機器内の回路部４との接続状態を示す図であって、（ａ）はスイッチ３がオン状態であり、（ｂ）はスイッチ３がオフ状態である。

【符号の説明】

１　上部カバー
１ａ　凸部
２　下部カバー
３　スイッチ
４　回路部

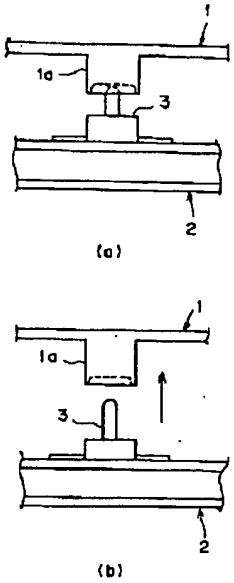
【図１】

本発明の一実施の形態に係る改ざん防止装置を組み込んだ電子機器を概略的に示した外観斜視図



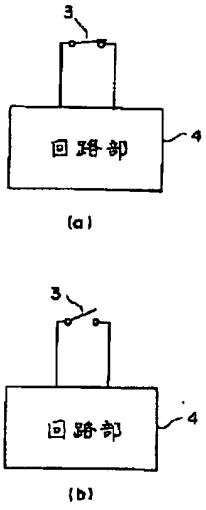
【図２】

図１に示したスイッチ３の動作を説明する図であって、(a)は上部カバー１を閉じた状態であり、(b)は上部カバー１を開いた状態である



【図３】

図１に示したスイッチ３と電子機器内の回路部４との接続状態を示す図であって、(a)はスイッチ３がオン状態であり、(b)はスイッチ３がオフ状態である。



フロントページの続き

(72)発明者　大庭　潤一郎
東京都稲城市矢野口1776番地　富士通機電株式会社内
(72)発明者　佐藤　誠
東京都稲城市矢野口1776番地　富士通機電株式会社内
(72)発明者　澤田　一郎
東京都稲城市矢野口1776番地　富士通機電株式会社内
(72)発明者　齊藤　智
東京都稲城市矢野口1776番地　富士通機電株式会社内

Fターム(参考)　5B017 AA07 BA08 CA14